PATENT APPLICATION
Docket No.: 45687-00036
P05139US00LH/maw

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of: Christian GEHRMANN et al.

For: METHOD AND ARRANGEMENT IN A   COMMUNICATION NETWORK

BOX PATENT APPLICATION
Commissioner of Patents
Washington, D.C. 20231

Sir:

PATENT APPLICATION TRANSMITTAL LETTER

Transmitted herewith for filing, please find the following:

1. (XX)   The specification of the above-referenced patent application is enclosed herewith (_22_ page(s) including claim(s) and Abstract).

2. (XX)   ___5_____ sheet(s) of:
___ informal drawing(s) is (are) enclosed herewith.
_X_ formal drawing(s) is (are) enclosed herewith.

3. ( )   This application is a:
___ Continuation
___ Divisional
___ Continuation-In-Part
of prior copending parent application
Serial No. _____ filed on _____, now pending.
Please amend the application to insert the following line in the beginning of the specification:
--This   application   is   a   Continuation   of   prior application Serial No. _____ filed on _____, now pending.--
In the event that a petition to extend time under 37 CFR 1.136 is necessary in the parent application to maintain copendency for this application, a petition for an extension of the necessary time to maintain copendency is hereby requested for the parent application and the Commissioner is hereby authorized to debt our Account Number 10-0447 for the necessary fees.

4. (X)   The fees for this application have been calculated and included as shown below (Prior to calculating the fees, please enter any enclosed preliminary amendment.):

	NO. FILED	NO. EXTRA	RATE	FEE
BASIC FEE				**$710**
TOTAL CLAIMS	38-20	18	$18	324
INDEPENDENT CLAIMS	2- 3	0	$80	0
MULTIPLE DEPENDENT CLAIM(S) PRESENTED			$270	270
TOTAL FEES:				**$1304.00**
Deduct one-half of fee for Small Entity				
TOTAL AMOUNT DUE:				**$1304.00**

   X   Checks in the amount of $1304.00 and $40.00 are enclosed herewith. Please charge any deficiency or credit any overpayment to Deposit Account No. _10-0447_ .

_____ Please charge my Deposit Account No. _____ in the amount of $_____. Please charge any deficiency or credit any overpayment to Deposit Account No. _____ .

5. (X)   An oath or declaration is enclosed herewith that is:
_____ Unsigned
  X   Newly executed per 37 CFR 1.63(a) and (b).
_____ A copy of the executed declaration filed in the prior application upon which priority is based, showing the signature or an indication thereon that it was signed; and:
     _____ This application is being filed fewer than all of the inventors named in the prior application and it is requested that the following name or names be deleted from the list of inventors in the prior application for this continuation or divisional application:

              _____

              _____ .

     _____ The prior application was accorded status under 37 CFR § 1.47 and is accompanied by:
          _____ A copy of the decision granting a petition to accord Sec. 1.47 status to the prior application (unless all of the inventors have or legal representatives have filed an oath or declaration to join in the prior application).

          ____   A copy of the subsequently executed oath(s) or declaration(s) filed by the inventor(s) or legal representative(s) that have subsequently joined in the prior application.

6. (X)   The power of attorney for this application:

       <u>X</u>   is appointed in the newly executed Oath or Declaration submitted herewith.

       ___   is appointed by the power of attorney enclosed herewith.

       ___   remains the same as originally in the parent application.

       ___   was changed during the prosecution of the parent application and a copy of the change in the power of attorney is enclosed herewith.

7. (XX)   The correspondence address for this application shall be:

               Richard J. Moura, Esq.

               Jenkens and Gilchrist, P.C.

               3200 Fountain Place

               1445 Ross Ave.

               Dallas, Texas 75202

       <u>X</u>   which is a new correspondence address or a change therein.

       ___   which is the same as originally in the parent application.

       ___   which is the change in the correspondence address that was filed during the prosecution of the parent application.

8. (XX)   Priority is hereby claimed under 35 USC 119 and 172 to the following foreign applications:

Country	Serial No.	Date
EPO	99850158.9	Oct. 27, 1999

    and:

       ___   A certified copy of each application is enclosed herewith.

       ___   A certified copy of each application was filed in prior application Serial No. _____.

9. ( )   A verified statement claiming small entity status under 37 CFR 1.9 and 1.27:

       ___   is enclosed herewith.

       ___   was filed in parent application Serial No. _____, and such status remains unchanged and is requested for this application.
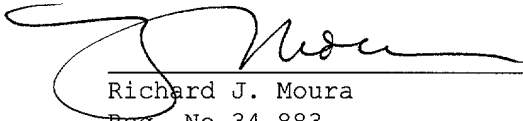
10. ( )   A preliminary amendment is enclosed herewith.

11. (XX)   An Information Disclosure Statement with Modified PTO Form 1449 and a copy of the cited references are enclosed herewith.

12. (XX)   An Assignment of the invention to <u>Telefonaktiebolaget LM Ericsson</u> with cover sheet and recordation fee is enclosed herewith for recordation by the Assignment Branch.

13. (XX)   The Commissioner is hereby authorized to charge payment, or to credit any overpayment, of the following fees associated with this

filing or during the pendency of this application to Deposit Account No. 10-0447.

  X   Any patent application filing fees under 37 CFR 1.16.

  X   Any patent application processing fees under 37 CFR 1.17.

       The issue fee under 37 CFR 1.18 at or before mailing of the Notice of Allowance, pursuant to 37 CFR 1.311(b).

14. ( )   Other (specify):_____

_____

_____.

15. (XX)   Confirmation Postcard.

Respectfully submitted,

Richard J. Moura
Reg. No.34,883

Jenkens & Gilchrist, P.C.
3200 Fountain Place
1445 Ross Avenue
Dallas, Texas 75202-2799
214/855-4709
214/855-4300 (Fax)

METHOD AND ARRANGEMENT IN A COMMUNICATION NETWORK

5   **FIELD OF INVENTION**

The present invention relates to the field of communication networks and more specifically to an ad hoc communication network and a method for establishing security in an ad hoc network.

10   **DESCRIPTION OF RELATED ART**

The fast growth of open networks with easy access has raised many security problems. Several security solutions for public networks like the Internet have appeared. Security is a problem in all kinds of open networks both wired and wireless. Information transmitted over the air is extremely vulnerable. Today there exist solutions that are built upon some type of so called *public key infrastructure* (PKI). A public key infrastructure is a system used to distribute and check public keys that can be used to authenticate users, exchange session keys, sign information or encrypt information.

20   In a PKI system, two corresponding (also called asymmetric) keys are used in connection with protecting information. Information, which is encrypted with one of the two keys, can be decrypted only with the other key. In some PKI systems either of the two keys can be used to encrypt and the other to decrypt. In other systems, one key must be used only for encryption and the other for decryption.

25   One important feature of PKI systems is that it is computationally unfeasible to use knowledge of one of the keys to deduce the other key. In a typical PKI system, each of the systems possesses a set of two such keys. One of the keys is maintained private while the other is freely published. If a sender encrypts a message with the recipient's public key, only the intended recipient can decrypt the

30   message, since only the recipient is in possession of the private key corresponding to the published public key. If the sender, before performing the above

encryption, first encrypts the message with the senders private key, the recipient, upon performing first a decryption, using the recipient's private key, then a decryption on the result, using the sender's public key, is assured not only of privacy but of authentication since only the sender could have encrypted a

5   message such that the sender's public key successfully decrypts it. In one digital signature scheme, one-way hash is first applied to a message and the hash of the message is encrypted with the sender's private key.

A PKI distributes one or several public keys and determine whether a certain

10   public key can be trusted for certain usage or not. A piece of digitally signed information is often called a certificate. Certificates are the basis upon which PKIs are built.

The degree of confidence that the recipient has in the source of a message depends on the degree of the recipient's confidence that the sender's public key

15   corresponds to a private key that was possessed only by the sender. In many current systems, a number of generally well trusted certification authorities have been established to provide this degree of confidence.

A common certificate format is Standard X.509 (developed by the International Standards Organisation (ISO) and the Comité Consultatif Internationale

20   Telegraphique et Telephonique (CCITT)). Such a certificate may, e.g., include a public key, the name of subject who possesses or is associated with the public key, an expiration date, all of which are digitally signed by a trusted party. The digital signature may be provided e.g., according to the digital signature standard (DSS) (National Institute of Standards and Technology (NIST)). Typically a digital

25   signature involves applying a one-way hash and then encrypting with the private key of, in this case, the certification authority. Such digital signature is provided using the private key of the trusted party which, in turn, is authenticated using the trusted party's certificate signed by yet another trusted party, so that there may be a multi-level hierarchy of trusted parties.

30   Another certificate format is Pretty Good Privacy (PGP) developed by P. Zimmermann and described in Internet Engineering Task Force (IETF) Open

PGP Specification. PGP provides a way to encrypt and decrypt, sign data and exchange keys. Thus it is more than just a PKI. However, the main idea with PGP is that no strict PKI is needed. Instead the PGP users themselves create and extend the PKI they need. This is done by certifying other users

5 public keys, i.e., signing trusted public keys with their own secret key. In this way a "web of trust" is created. A particular key may have several different user IDs. Typically a user ID is an email address. If a revocation signature follows a key, the key is revoked. A user certifies another users key by signing it with one of the keys of his own, which has signing capability.

10 When signing another key, different trust levels can be set, i.e., the amount of confidence the signer has in the signed key and user ID.

Today, so-called ad hoc networks are used more and more frequently. An ad hoc network is established temporary for a special purpose. There is no fixed

15 infrastructure, the nodes are the network. The nodes within the network are often mobile and using radio links. An ad hoc network might constitute dynamic wide area connectivity in situations such as military operations, rescue and recovery operations, and remote construction sites. An ad hoc network might also constitute local area connectivity in situations such as temporary conference sites,

20 home networks and robot networks. An ad hoc network might also constitute personal area networks in situations such as interconnected accessories, ad hoc conference table and games. The nodes might consist of e.g. mobile phones, lap tops, television sets, washing machines In some situations like in military operations or business conferences when the communication between the nodes

25 comprises secrets, it is very important that a sender of a message can trust that the receiver really is the intended receiver.

In the previous examples, bindings between public keys and names or authorisation are described. Several of these certificate solutions exist in different

30 systems. However, it is not yet described how different certificates needed for different kinds of purposes are obtained. In the case of ordinary X.509 type of

PKI with hierarchical Certificate Authority (CA) structures, finding the right certificate is done using some central on-line server or by direct transmission of the certificate at connection set up. When using PGP either the desired public key is stored locally on a machine or the device has to make a connection to a central PGP server in order to find the desired pubic key. This works if it is possible for entities that need some type of security relation to have on-line connections to some particular servers. This is not the case for ad hoc networks. Ad hoc networks are created on the fly between entities that happen to be at the same physical location.

Therefore, what is further needed is a mechanism for checking if different nodes in an ad hoc network share a trust relation and for creating trust among a certain set of nodes without any pre-defined relations.

The problem of how to distribute trust using public keys in ad hoc networks is addressed in this invention. Still the existing PKIs provide a basis upon which solution also for ad hoc network can be built.

SUMMARY OF THE INVENTION

The present invention relates to the requirement of security in an ad hoc network. More particularly it relates to the problem within ad hoc networks, not having on-line connections to a particular server for getting desired public keys or certificates, required to create trust relations.

Accordingly, it is an object of the present invention to unravel the above-mentioned problem.

The aforesaid problem are solved by means of a method for finding possible trust relations between nodes within the ad hoc network and share them with other nodes within the ad hoc network.

5   The following scenario of establishing security in an ad hoc network describes the inventive concept of the present invention.

Within an ad hoc communication network, some of the nodes have a mutual trust relation to each other, thus constituting a trust group. A node within the network

10   is being a candidate node for joining the trust group. An X-node is identified, being a member of a trust group and having a trust relation with the candidate node. The X-node distributes trust relations between the members of the trust group and the candidate node.

15   An advantage of the present invention is it is possible to achieve the necessary security associations needed for distributing and sharing information among a group of users that happens to be at the same physical location. There are a large amount of applications that fits in to this scenario. Among those can be mentioned people from different companies or organisations that gather in a

20   conference room can share documents with the meeting members.

Another advantage of the present invention is that the number of manually created trust relations between members in an ad hoc communication network is decreased.

25

Further scope of applicability of the present invention will become apparent from the detailed description given hereinafter. However, it should be understood that the detailed description and specific examples, while indicating preferred embodiments of the invention, are given by way of illustration only, since various

30   changes and modifications within the spirit and scope of the invention will become apparent to those skilled in the art from this detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

DESCRIPTION OF PREFFERED EMBODIMENTS

The ad hoc communication network according to the invention constitutes e.g. a bluetooth network. The ad hoc network comprises nodes constituting e.g., laptops and mobile phones, each node comprising a receiver and a computer, the computer comprising a processor and a memory. The nodes are interconnected via communication links.

Figure 1 shows a possible scenario of the present invention in which a single node 101 is added to an existing trust group 102. The trust group 102 comprises nodes 103-105. All the nodes 103-105 in the trust group 102 have mutual trust relations with each other, the trust relations being created with trusted public keys. Thus each node 103-105 in the trust group 102 has the trusted public keys of all

the other nodes 103-105 within the trust group 102. The trusted public keys are e.g. used to sign messages to be sent between trusted nodes. The single node 101 and the trust group constitute an ad hoc communication network 106. According to the invention all nodes 101, 103-105 have authority to delegate trust to other nodes that they trust within the network. The single node 101 would like to join the trust group 102 and the single node is from now on called the candidate node 101.

Either the candidate node 101 sends a broadcast message to all the nodes 103-105 within the trust group or it unicasts message to a special look up server where all the nodes 103-105 can obtain the message. The message comprises the public key that the candidate node 101 wants to use. The message might comprise a set of public keys that the candidate node 101 wants to use and possible certificate/s certifying the public key/s.

Each node 103-105 within the trust group 102 obtains the public key of the candidate node 101, and checks if it trusts the public key of the candidate node.

A node 103 within the trust group that trusts the public key of the candidate node 101 is identified, a so-called X-node 103. The X-node,

- sends a signed message comprising all the trusted keys of the nodes 103-105 within the trust group 102 to the candidate node 101, and

- signs the public key of the candidate node 101 and sends a message comprising the key together with the signature to all the other nodes 104, 105 within the trust group 102.

If none of the nodes 103-105 within the trust group 102 trusts the candidate node a trust relation has to be manually created with an arbitrary node 105 within the trust group 102. This node 105 thus constitutes an X-node. A manual creation of trust relation between two nodes can be performed in different ways. In one way the two nodes enter their pin codes and then exchange public keys using an

authenticated channel. The manual creation of trust relations results in that each node obtains a trusted public key from the other party.

After the manual creation of trust, the X-node 105

5   —   sends a signed message comprising all the trusted keys of the nodes 103-105 within the trust group 102 to the candidate node 101, and

    —   signs the public key of the candidate node 101 and sends a message comprising the key together with the signature to all the other nodes 103, 104 within the trust group 102.

10

Figure 2 shows another scenario of the present invention. In this scenario an ad hoc communication network 201 is formed. The trust groups 202, 203, 204 and 205 within the ad hoc network are used to create additional trust relations within

15 the network. The trust relations are created with signed public keys. The ad hoc network comprises nodes A-M. In this embodiment, each of the nodes A-M constitutes a node being a candidate for joining a secure ad hoc network i.e., a trust group wherein all nodes A-M have mutual trust relations.

20 The nodes A, B, C, D and E have mutual trust relations and constitute a trust group 202.

The nodes D, E, G, J and K have mutual trust relations and constitute a trust group 203.

The nodes A, E, F and I have mutual trust relations and constitute a trust group

25 204.

The nodes H and M have mutual trust relations and constitute a trust group 205.

The node L has no trust relations to any of the other nodes within the network.

As shown in figure 2, the node E belongs to three trust groups 202, 203 and 204.

30 The node D and E belong to two trust groups, 202 and 203. The nodes A and E belong to two trust groups 202 and 204.

According to the invention all nodes A-M have authority to delegate trust to other nodes that they trust, within the network. 201.

5 Each node A-M within the ad hoc network 201 sends a broadcast message to all the nodes A-M within the ad hoc network 201 or a unicast message to a special look up server where all the nodes A-M can obtain the message. The message comprises the public key that the candidate node A-M wants to use. The message might comprise a set of public keys that the candidate node wants to use and

10 possible certificate/s certifying the public key/s.

Each of the nodes A-M obtains the public keys of all the other nodes A-M, either they are trusted or untrusted. Each node A-M then creates a list of its trusted nodes and their corresponding keys. E.g. node A which belongs to trust group

15 202 trusts the nodes B, C, D and E.

In this scenario, one node A is decided to act as a server node A. Each of the nodes B-M, sends a registration message to the server node A comprising its public key and the list of its trusted nodes and their corresponding public keys.

20 Using the obtained information the server node A identifies all the nodes A-M and the trust groups 202-205 within the ad hoc network.

Server node A might find that some nodes or some trust groups are isolated, i.e.

25 neither having a trust relation with the server node A nor having a trust relation with any of the nodes that A has a trust relation with. In this embodiment that goes for node L and trust group 205 comprising the nodes H and M.

In that case server node A asks the node L, to manually create a trust relation with

30 the server node A. Server node further A asks one node H in that trust group 205, to manually create a trust relation with the server node A. This results in two more

trust groups and is illustrated in **figure 3**. The nodes A and L constitutes trust group 301 and the nodes A and H constitutes trust group 302.

5 The server node A classifies all the nodes within the ad hoc network as being nodes that the server node A trusts, nodes B, C, D, E, F, I, H and L, i.e. sever-trusted nodes, or as being nodes that server node A not trust, nodes G, J, K and M, i.e. server-untrusted nodes. The server node A then makes a list comprising the server-untrusted nodes, the so-called untrust-list.

10 A server-trusted node trusting a server-untrusted node constitutes a so-called Y-node. The server node A identifies as many Y-nodes as required for distributing trust relations to all or as many as possible of the server-untrusted nodes. I.e. server node A identifies node D, having trust relations with nodes G, K and J, and node H having a trust relation with node M. Thus node D and node H can

15 distribute trust relations between all the server-untrusted nodes and server node A according to the following process:

The server node A sends a message to the identified Y-nodes, the message comprising,

20 — the untrust-list comprising the nodes G, J, K and M and their corresponding public keys, and

— a request of distributing as many trust relations as possible between server node A and server-untrusted nodes.

25 An Y-node obtains the message and checks, which of the keys it trusts, i.e. which of the server-untrusted nodes G, J, K and M the Y-node trusts.

The identified Y-nodes then each perform the following steps 1-3 for each of the nodes that the respective Y-node trusts. In this case the Y-node D performs the

30 steps for each of the nodes G, J and K and Y-node H performs the steps for node M.

1. The Y-node signs the public key of server node A and sends it to the node that the Y-node trusts, e.g. Node D signs server node A's key and sends it to node G,

2. The Y-node signs the public key of the node that the Y-node trusts and sends
5   it to server node A, e.g. Node D signs node G's key and sends it to server node A.

3. Server node A reclassifies the node that the Y-node trust, and that the server node A now trusts, as now being a server-trusted node, and the untrust-list is reduced with said node, e.g. server node A reclassifies node G as being a server
10 trusted node and the untrust-list is reduced to J, K, and M.

The distribution of trust relations is now completed and the untrust-list is empty. Server node A has collected signed public keys from all nodes B-M within the ad hoc network 201 and sends a message to all nodes B-M comprising server node
15 A's collected signed public keys from all the nodes B-M within the ad hoc network.

The nodes A-M within the ad hoc communication network 201 now have mutual trust relations and a secure ad hoc network is established.
20

Figure 4 shows yet another scenario of the present invention. In this scenario an ad hoc network 401 comprises two trust groups 402 and 403 which shall be merged to one trust group constituting a secure ad hoc network. The first trust
25 group 402 comprises a set of nodes, N, O, P, Q and R, all having mutual trust relations. The second trust group 403 comprises a set of nodes, S, T, U, V and W, all having mutual trust relations and which all are candidate nodes for joining the first trust group 402. The trust relations are created with trusted public keys. A node P is decided to act as a server node P within the first trust group 402 and a
30 candidate node S is decided to act as a server node S within the second trust

group. According to the invention, the nodes N-W are authorised to delegate trust relations to other nodes within the network that it trusts.

Server node S sends a message, comprising a list of all candidate nodes S, T, U, V and W within the second trust group 403 and their corresponding public keys, to server node P. First server node P checks if it trusts any of the obtained keys, i.e. if it has trust relations to any of the candidate nodes S, T, U, V and W. First server node P, then classifies the candidate nodes as being first server-trusted nodes or as being first server-untrusted node, in this case P-trusted or P-untrusted.

If the classification results in at least one first server-trusted node, a scenario comes up as illustrated in **figure 5**. In this scenario first server node P has a trust relation to the node W and first server node P sends a message to second server node S. The message comprises

— a list of all nodes N, O, P, Q and R within the first trust group 402 and their corresponding public keys, and

— a list of first server-trusted nodes, which in this case is the P-trusted node W, and its corresponding public key.

Second server node S obtains the message and signs it and forwards it to node W.

Node W receives the signed message and checks the signature of the message. If node W trusts the signature, node W

— signs the received public keys of the nodes N, O, P, Q and R within the first trust group 402,

— sends a signed message comprising the signed public keys of the nodes N, O, P, Q and R within the first trust group 402 to all candidate nodes S, T, U and V within the second network,

— sends a signed message comprising all trusted public keys of the candidate nodes S, T, U, V and W to first server node P.

First server node P receives the message and checks the signature of the message. If it is valid, first server node P signs the public keys of the candidate nodes S, T, U, V and W within the second trust group 403 and sends them in a signed message to all nodes N, O, Q and R.

The nodes N-W within the ad hoc network 102 now have mutual trust relations and a secure ad hoc communication network is established.

In another scenario, shown in **figure 6**, the classification is resulting in no first server-trusted node i.e. a P-trusted node. This means that first server node P has no trust relation with any of the candidate nodes S, T, U, V and W. Server node P then asks the other nodes N, O, Q and R within the first trust group 402, one by one, until sever node P obtains a positive answer of the question, if they have a trust relation with any of the candidate nodes S, T, U, V and W, within the second trust group 403.

In this case, node N has no such trust relation, the query is forwarded to node O, which has not got such trust relation either. The query is forwarded to node Q, which has a trust relation with node V in the second trust group, and now the procedure of distributing trust can start.

Node Q sends a signed message to second server node S. The message comprises:

- a list of all nodes N, O, P, Q and R within the first trust group 402 and their corresponding public keys,
- a list of the nodes that node Q trusts, which in this case is the node V, and its corresponding public key.

Second server node S obtains the message and forwards it to node V.

Node V receives the signed message and checks the signature of the message. If node V trusts the signature, it signs the received public keys of the nodes N, O, P, Q and R within the first trust group 402. Node V then sends a signed message comprising the signed public keys of the nodes N, O, P, Q and R within the first

5   trust group 402 to all candidate nodes S, T, U and W within the second network. Node V sends a signed message comprising all trusted public keys of the candidate nodes S, T, U, V and W to node Q.

Node Q receives the message and checks the signature of the message. If it is

10   valid, node Q signs the public keys of the candidate nodes S, T, U, V and W within the second trust group 403 and sends the keys in a signed message to the other nodes N, O, P and R within the first trust group 402.

The nodes N-W within the ad hoc network 102 now have mutual trust relations

15   and a secure ad hoc communication network is established.

In yet another scenario, none of the nodes N, O, P, Q and R, within the first trust group 402, have a trust relation with any of the candidate nodes S, T, U, V and W,

20   within the second trust group 403. In this case a message is returned to first server node P asking node P to manually create a trust relation with the second server node S. This scenario is illustrated in **figure 7**. First server node P and second server node S now constitute a trust group 701.

25   First server node P sends a message to second server node S. The message comprises a list of all nodes N, O, P, Q and R, within the first trust group 402, and their corresponding public keys.

Second server node S

30   — signs the received public keys of the nodes N, O, P, Q and R within the first trust group 402,

— sends a signed message comprising the signed public keys of the nodes N, O, P, Q and R within the first trust group 402 to all candidate nodes S, T, U and V within the second network,

— sends a signed message comprising all trusted public keys of the candidate

5   nodes S, T, U, V and W to first server node P.

First server node P receives the message and checks the signature of the message. If it is valid, first server node P signs the public keys of the candidate nodes S, T, U, V and W within the second trust group 403 and sends them in a signed

10   message to all nodes N, O, Q and R.

The nodes N-W within the ad hoc communication network 102 are now having mutual trust relations and a secure ad hoc network is established.

15

CLAIMS

1. Method for establishing security in an ad hoc communication network (106), the ad hoc network (106) comprising a set of communication nodes (101, 103-105) whereof at least two of the nodes (103-105) having a mutual trust relation and thus constituting a trust group (102), the trust relations being created with public keys, and at least one additional node (101), being a candidate for joining the trust group (102) within the ad hoc network (106), **characterised** by the nodes having authority to delegate trust to nodes they trust, the method comprising the steps of

   – a) identifying a node (103) within the trust group having a trust relation with the candidate node (101), a so-called X-node (103);

   – b) distributing trust relations between all the members in the trust group (102) and the candidate node (101) by means of the X-node (103).

2. The method of claim 1, **characterised** by comprising the further step to be taken before step a), the candidate node (101) sending a message, comprising its public key, to all nodes (103-105) within the network.

3. The method of any of the previous claims, **characterised** in that the ad hoc network (106) comprises a single trust group (102), and a single candidate node (101), wherein step b), implies that the X-node (103) sends a signed message, comprising a list of the nodes (104, 105) that the X-node (103) trusts within the ad hoc network (106), and all their corresponding public keys, to the candidate node (101).

4. The method according to any of the previous claims, **characterised** in that step b) further implies that the X-node (103) signs the candidate node's (101) public key.

5. The method according to the previous claim, **characterised** in that step b) further implies, the X-node (103), sends a message, comprising the candidate node's (101) signed public key, to the nodes (104-105) within the trust group (102).

5

6. The method according to claim 2 **characterised** in that the ad hoc network (201) comprises a set of nodes (A-M) comprising several trust groups (202-205), and all nodes (A-M) being candidates for joining all trust groups, within the ad hoc network, that they are not already a member of, the method comprising the further step to be taken, by each node (A-M), after receiving the messages from all candidate nodes (A-M),

creating a list of the candidate nodes that the particular node trusts and their corresponding public keys.

7. The method according to the previous claim, **characterised** by further comprising the step of deciding one node (A) within the ad hoc network (201) to act as a server node (A).

8. The method according to any of the claims 6-7, **characterised** by further comprising the step of, the server node (A) receiving from each other node (B-M) within the network, a message comprising its respective public key, the respective list of the candidate nodes that the respective node trust and their corresponding public keys.

9. The method according to the previous claim, **characterised** by further comprising the step of, the server node (A) *classifying* the at least one candidate node as being a server-trusted node (B, C, D, E, F and I) or as being a server-untrusted node (G, H, J, K, L and M), depending on whether the server node (A) trusts it or not.

10. The method according to the previous claim, wherein a server-trusted node trusting a server-untrusted node constitutes a so-called Y-node, **characterised in** that the step a) implies that the server node (A) identifies at least one Y-node required for distributing trust relations between the server node (A) and as many server-untrusted nodes as possible.

11. The method according to the previous claim, **characterised in** step b) further implying that server node (A) sends a request to the identified Y-nodes (D, H) of distributing said trust relations between server node A and server-untrusted nodes.

12. The method according to the previous claim, **characterised in** step b) further implying that server node (A) obtains said requested trust relations.

13. The method according to the previous claim, **characterised in**, the step of obtaining the trust relations comprising that for each server-untrusted node that the Y-node have a trust relation with, the Y-node signs the public key of the server node (A) and forwards it to the server-untrusted node.

14. The method according to any of the claims 12-13, **characterised in** the step of obtaining the trust relations comprising that for each server-untrusted node that the Y-node have a trust relation with, the Y-node signs the public key of the server-untrusted node and forwards it to the server node (A).

15. The method according to any of the claims 12-14, **characterised by** comprising the further step of, server node (A), after obtaining said trust relation, reclassifying the server-untrusted node with the obtained trust relation as being a server-trusted node.

16. The method according to any of the claims 12-15, **characterised** by comprising the further step of, server node (A) sending a signed message comprising the server node's (A) all trusted public keys belonging to trusted candidate nodes within the ad hoc network. (201).

5

17. An ad hoc communication network (106) comprising a set of communication nodes (101, 103-105) whereof

the nodes (101, 103-105) each comprising a receiver and a computer, the computer comprising a processor and a memory,

10 the nodes (101, 103-105) being interconnected with communication links,

at least two of the nodes (103-105) are having a mutual trust relation and thus constituting a trust group (102), the trust relations being created with public keys, and

at least one additional node (101) being a candidate for joining at least one

15 trust group (102) within the ad hoc network,

characterised by

the candidate node (101) having means for requesting if any of the nodes within the trust group (102) have a trust relation with the candidate node (101),

20 the nodes being authorised to and are having means for, distributing trust relations between its trust group(102) and the candidate node (101) that it trusts.

18. The ad hoc communication network (201) according to the previous claim,

25 **characterised** by each node (A-M) having means for creating a list of the candidate nodes that the node trusts and their corresponding public keys, to be stored in the memory.

19. The ad hoc communication network according to any of the claims 17-18,

30 **characterised** in that one node (A) within the ad hoc network (201) being a server node (A), capable of administrate distribution of trust relations.

20. The ad hoc communication network (201) according to the previous claim, **characterised** by the server node (A) having means for classifying the at least one candidate node as being a server-trusted node (B, C, D, E, F and I), or as being a server-untrusted node (G, H, J, K, L and M), depending on whether the server node (A) trusts the candidate node or not.

21. The ad hoc communication network (201) according to the previous claim, wherein a server-trusted node trusting a server-untrusted node constitutes a so-called Y-node **characterised** by the server node (A) having means for identifying at least one Y-node (D, H) required for distributing trust relations between the server node A and the server-untrusted nodes.

22. The ad hoc communication network (201) according to the previous claim **characterised** by the server node (A) having means for sending to each of the identified Y-nodes (D, H),

   a request as to which of the server-untrusted nodes (G, H, J and M) the Y-node (D, H) has a trust relation with, and

   a request for distributing trust relations between the server node (A) and the requested server-untrusted nodes.

23. The ad hoc communication network according to any of the claims 20-22, **characterised** by the server node (A) having means for distributing obtained trust relations to the nodes within the ad hoc communication network (201).

24. A computer program product directly loadable into the internal memory of a digital computer within a node being a member of an ad hoc communication network, comprising software code portions for performing the steps of any of the claims 1-16 when said product is run on a computer.

25. A computer program product stored on a computer usable medium, comprising readable program for causing a computer, within a node being a member of an ad hoc communication network, to control an execution of the steps of any of the claims 1-16.

ABSTRACT

The present invention relates to the requirement of security in an ad hoc network.

5 More particularly it relates to the problem within ad hoc networks, not having on-line connections to a particular server for getting desired public keys or certificates, required to create trust relations.

Within an ad hoc communication network, some of the nodes have a mutual trust relation to each other, thus constituting a trust group. An additional node within

10 the network is being a candidate node for joining the trust group. An X-node is identified, being a member of a trust group and having a trust relation with the candidate node. The X-node distributes trust relations between the members of the trust group and the candidate node.
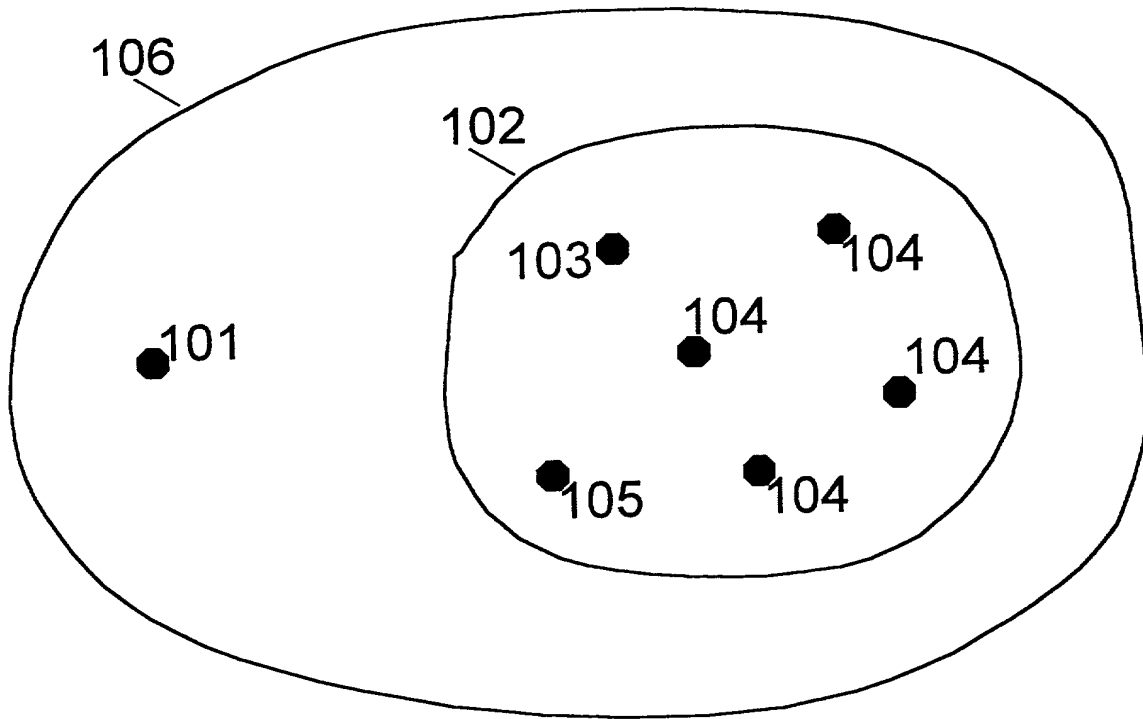
Fig. 1
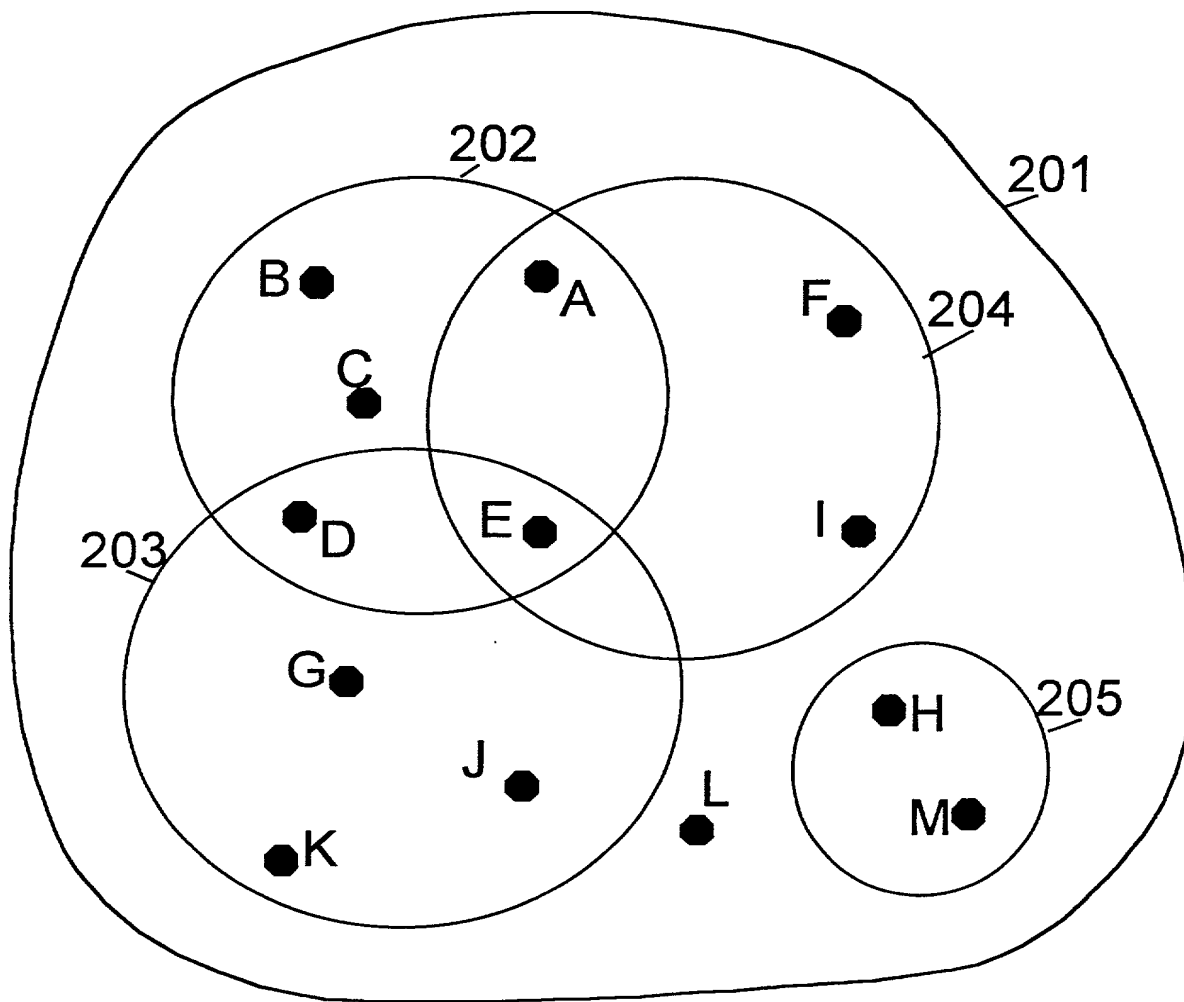
Fig. 2
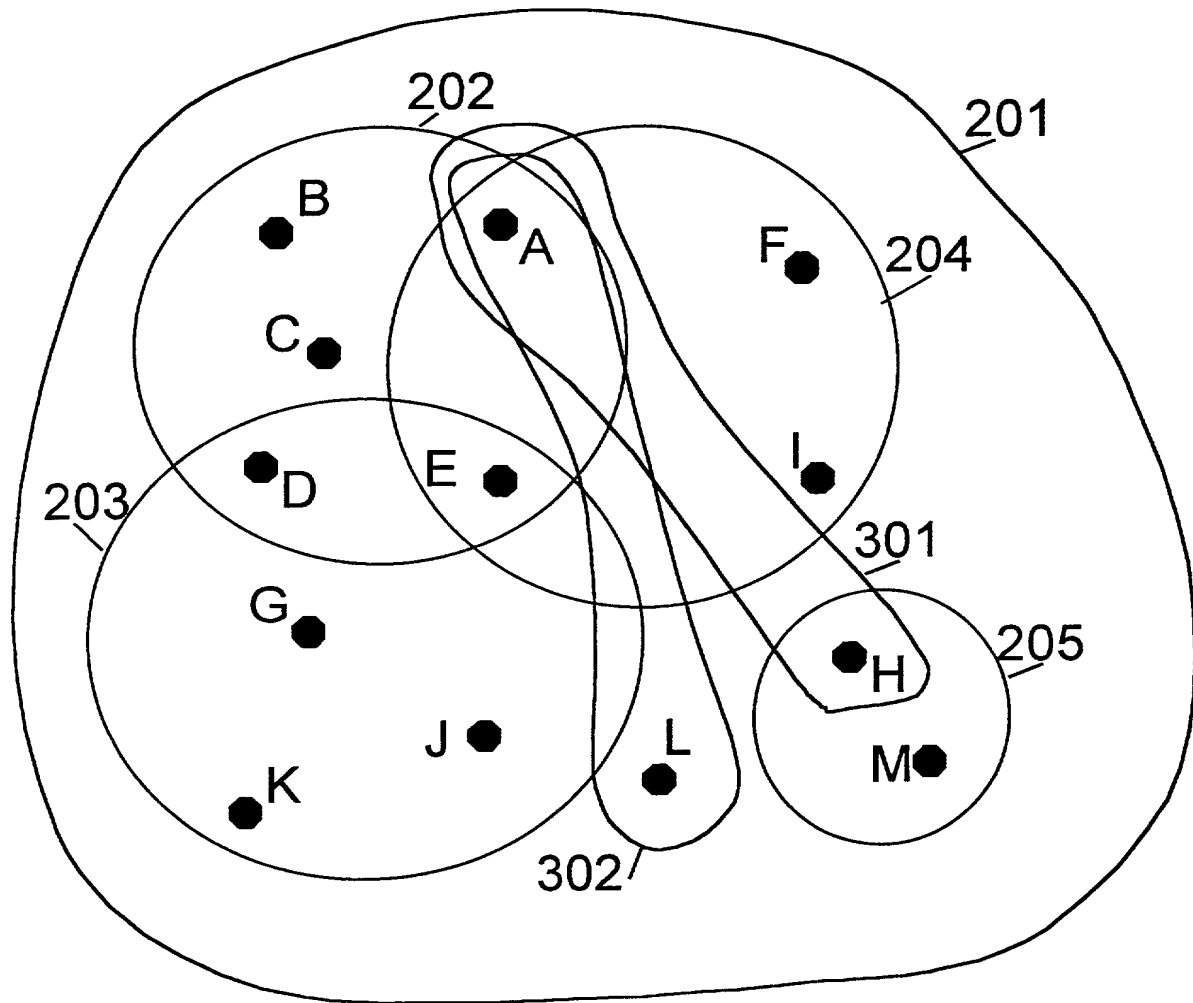
Fig. 3
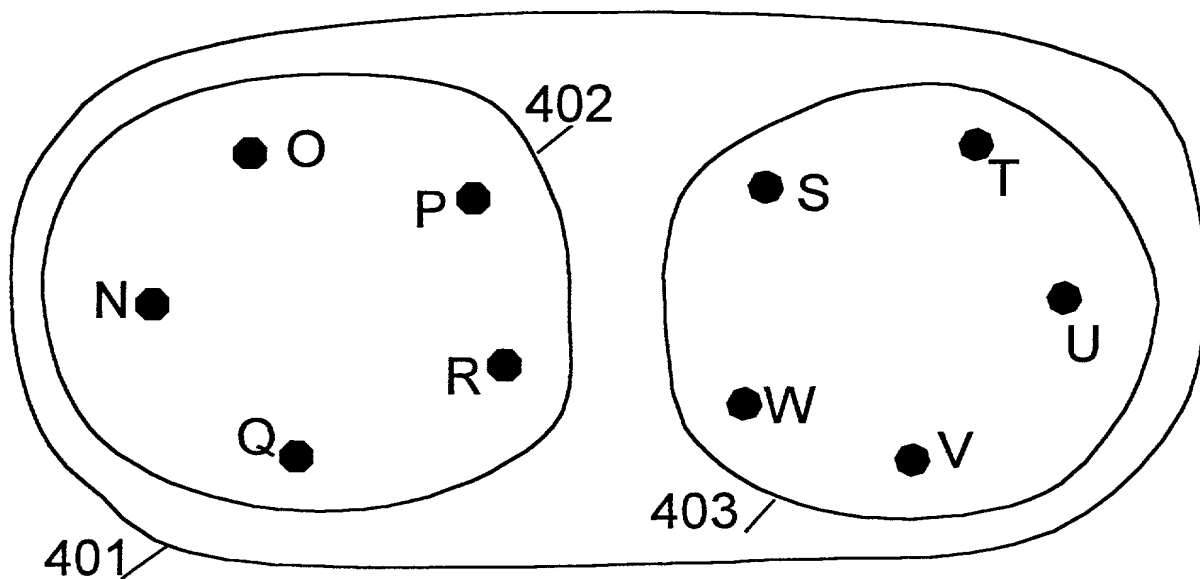
Fig. 4
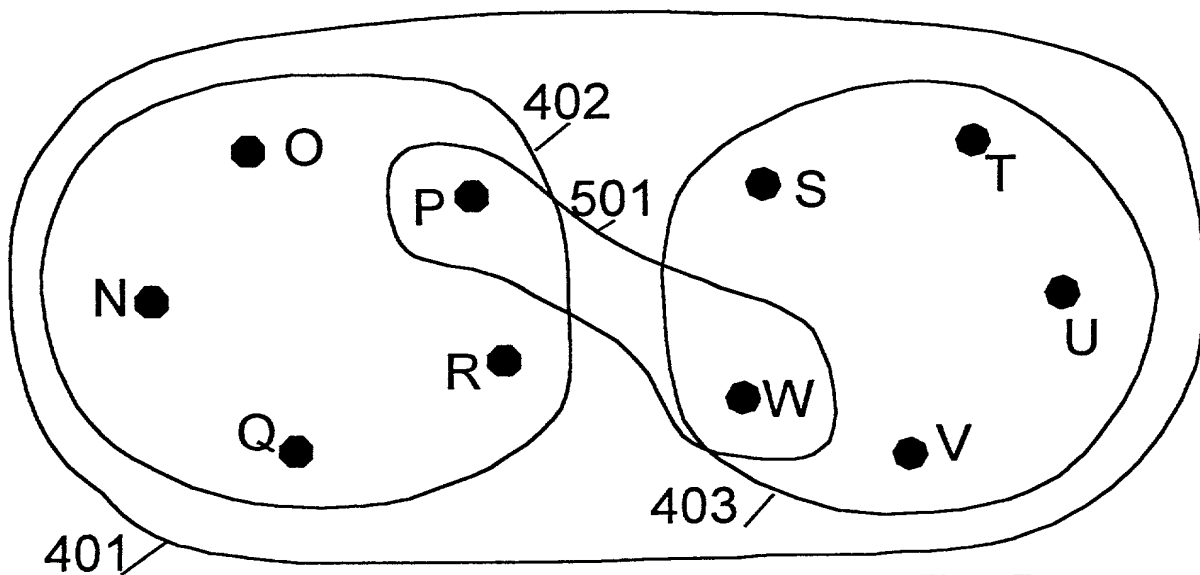
Fig. 5
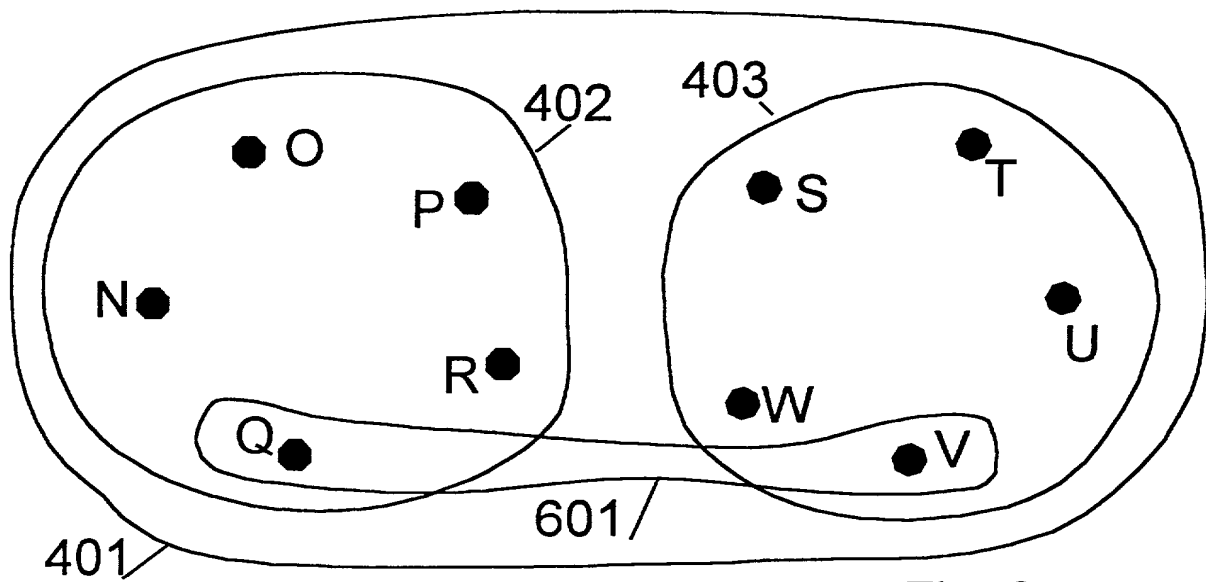
Fig. 6
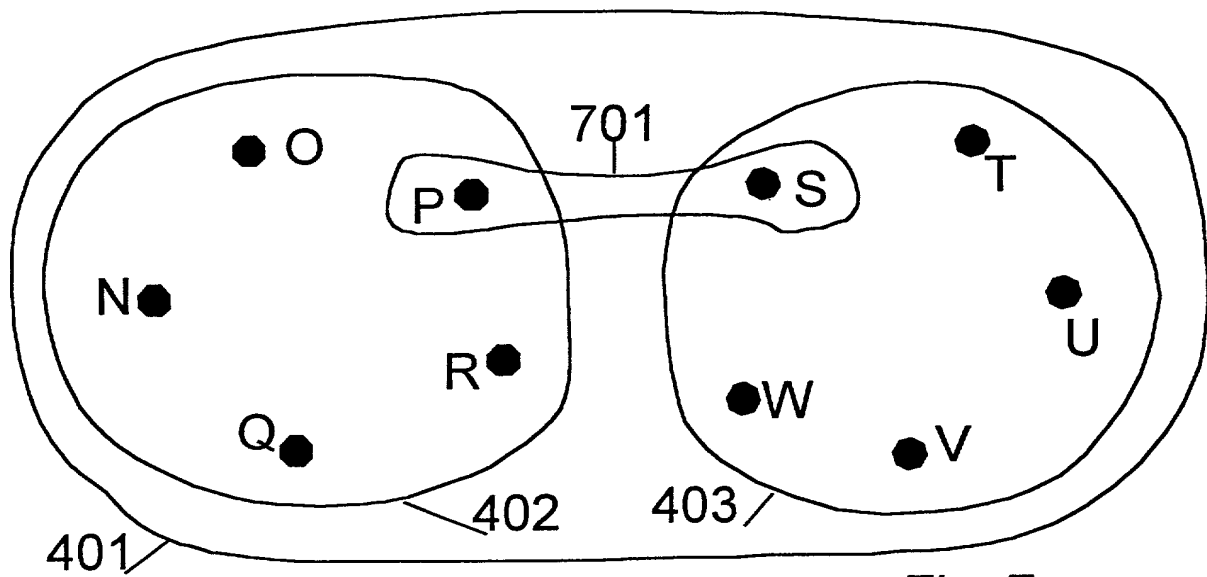
Fig. 7

RULES 63 AND 67 (37 C.F.R. 1.63 and 1.67)
DECLARATION AND POWER OF ATTORNEY

FOR UTILITY/DESIGN/CIP/PCT NATIONAL APPLICATIONS

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name; and

I believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD AND ARRANGEMENT IN A COMMUNICATION NETWORK.
_____,

the specification of which: (mark only one)

   __   (a)   is attached hereto.

   __   (b)   was filed on_ as Application Serial No. __ and was amended on _____ (if applicable)

   _   (c)   was filed as PCT International Application No. PCT/_____ on _____, _____ and was amended on _____ (if applicable).

   __   (d)   was filed on ___ as Application Serial No. ___ and was issued a Notice of Allowance on ___.

   __   (e)   was filed on ___ and bearing attorney docket number ___

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above or as allowed as indicated above.

I acknowledge the duty to disclose all information known to me to be material to the patentability of this application as defined in 37 CFR § 1.56. If this is a continuation-in-part (CIP) application, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose to the Office all information known to me to be material to patentability of the application as defined in 37 CFR § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

I hereby claim foreign priority benefits under 35 U.S.C. § 119/365 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate filed by me or my assignee disclosing the subject matter claimed in this application and having a filing date (1) before that of the application on which my priority is claimed or, (2) if no priority is claimed, before the filing date of this application:

PRIOR FOREIGN PATENTS

Number	Country	Month/Day/Year Filed	Date first laid-open or Published	Date patented or Granted	Priority Claimed Yes	No
99850158.9	EP	10.27.99			X	

I hereby claim the benefit under 35 U.S.C. § 120/365 of any United States application(s) listed below and PCT international applications listed above or below:

PRIOR U.S. OR PCT APPLICATIONS

Application No. (series code/serial no.)	Month/Day/Year Filed	Status(pending, abandoned, patented)

I hereby appoint:

TIMOTHY G ACKERMANN, Reg No 44,493
THOMAS E ANDERSON, Reg No 37,063
BENJAMIN J BAI, Reg No 43,481
MICHAEL J BLANKSTEIN, Reg No 37,097
MARY JO BOLDINGH, Reg No 34,713
MARGARET A BOULWARE, Reg No 28,708
ARTHUR J BRADY, Reg No 42,356
MATTHEW O BRADY, Reg No 44,554
DANIEL J BURNHAM, Reg No 39,618
THOMAS L CANTRELL, Reg No 20,849
RONALD B COOLLEY, Reg No 27,187
THOMAS L CRISMAN, Reg No 24,846
STUART D DWORK, Reg No 31,103
WILLIAM F ESSER, Reg No 38,053
ROGER J FRENCH, Reg No 27,786
JANET M GARETTO, Reg No 42,568
JOHN C GATZ, Reg No 41,774
RUSSELL J GENET, Reg No 42,571

J KEVIN GRAY, Reg No 37,141
STEVEN R GREENFIELD, Reg No 38,166
J PAT HEPTIG, Reg No 40 643
SHARON A ISRAEL, Reg No 41,867
JOHN R KIRK JR , Reg No 24,477
PAUL R KITCH, Reg No 38,206
TIMOTHY M KOWALSKI, Reg No 44,192
JAMES F LEA III, Reg No 41,143
ROBERT W MASON, Reg No 42,848
ROGER L MAXWELL, Reg No 31,855
ROBERT A McFALL, Reg No 28,968
STEVEN T McDONALD, Reg No 45,999
LISA H MEYERHOFF, Reg No 36,869
STANLEY R MOORE, Reg No 26,958
RICHARD J MOURA, Reg No 34,883
MARK V MULLER, Reg No 37,509
P WESTON MUSSELMAN JR Reg No 31,644
SPENCER C PATTERSON, Reg. No 43,849

RUSSELL N RIPPAMONTI, Reg No 39 521
STEPHEN G RUDISILL, Reg No 20 087
HOLLY L RUDNICK, Reg No 43 065
J L JENNIE SALAZAR, Reg No 45,065
KEITH W SAUNDERS, Reg No 41,462
JERRY R SELINGER, Reg No 26,582
KEVIN J SIMONS, Reg No 45,110
GARY B SOLOMON, Reg No 44,347
WAYNE O STACY, Reg No 45,125
STEVE Z SZCZEPANSKI Reg No 27,957
ANDRE M SZUWALSKI, Reg No 35,701
ALAN R THIELE, Reg No 30,694
TAMSEN VALOIR, Reg No 41,417
RAYMOND VAN DYKE, Reg No 34,746
BRIAN D WALKER, Reg No 37,751
GERALD T WELCH, Reg No 30,332
HAROLD N WELLS, Reg. No 26,044
WILLIAM D WIESE, Reg No 45,217

all of the firm of **JENKENS & GILCHRIST, a Professional Corporation**, 1445 Ross Avenue, Suite 3200, Dallas, Texas 75202-2799, as my attorneys and/or agents, with full power of substitution and revocation, to prosecute this application, provisionals thereof, continuations, continuations-in-part, divisionals, appeals, reissues, substitutions, and extensions thereof and to transact all business in the United States Patent and Trademark Office connected therewith, to appoint any individuals under an associate power of attorney and to file and prosecute any international patent application filed thereon before any international authorities, and I hereby authorize them to act and rely on instructions from and communicate directly with the person/assignee/attorney/firm/organization who/which first sent this case to them and by whom/which I hereby declare that I have consented after full disclosure to be represented unless/until I instruct them in writing to the contrary.

Please address all correspondence and direct all telephone calls to:

Richard J. Moura, Esq.
Jenkens & Gilchrist, P.C.
1445 Ross Avenue, Suite 3200
Dallas, Texas 75202-2799
214/855-4500
214/855-4300 (fax)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAMED INVENTOR(S)

1	Christian Gehrmann		*[signature]*	9.27.2000
	Full Name		**Inventor's Signature**	**Date**
	S:t Månsgatan 17 A		Swedish	
	Residence (city, state, country)		**Citizenship**	
	S-222 29 LUND, Sweden			
	Post Office Address (include zip code)			

(FOR ADDITIONAL INVENTORS, check here X and add additional sheet for inventor information regarding signature, name, date, citizenship, residence and address)

2	Rolf Blom **Full Name**	*[signature]* **Inventor's Signature**	9.27.2000 **Date**
	Svärdvägen 2 **Residence** (city, state, country)	Swedish **Citizenship**	
	S-175 68 JÄRFÄLLA, Sweden **Post Office Address** (include zip code)		